CLAIMS

What is claimed is:

1. A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications;

(d) executing a pattern for testing the potentially malicious content network communications for malicious code; and

(e) conditionally delivering the network communications over the network based on the testing.

2. The method as recited in claim 1, further comprising scanning the network communications for known malicious content.

3. The method as recited in claim 1, wherein the malicious content includes a mass-mailer virus.

4. The method as recited in claim 1, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

5. The method as recited in claim 1, wherein the network communications include electronic mail messages.

6. The method as recited in claim 5, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

7. The method as recited in claim 1, wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

8. The method as recited in claim 1, further comprising cleaning the potentially malicious content if malicious code is found for disabling the malicious code.

9. A computer program product for network-based scanning for potentially malicious content, comprising:

(a) computer code that monitors network communications over a network;

(b) computer code that identifies potentially malicious content in the network communications;

(c) computer code that quarantines the potentially malicious content of the network communications;

(d) computer code that executes a pattern for testing the potentially malicious content network communications for malicious code; and

(e) computer code that conditionally delivers the network communications over the network based on the testing.

10. A system for network-based scanning for potentially malicious content, comprising:

(a) logic that monitors network communications over a network;

(b) logic that identifies potentially malicious content in the network communications;

(c) logic that quarantines the potentially malicious content of the network communications;

(d) logic that executes a pattern for testing the potentially malicious content network communications for malicious code; and

(e) logic that conditionally delivers the network communications over the network based on the testing.

11. A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications; and

(d) delivering the network communications over the network after a predetermined delay.

12. The method as recited in claim 11, further comprising scanning the network communications for known malicious content.

13. The method as recited in claim 11, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

14. The method as recited in claim 11, wherein the network communications include electronic mail messages.

15. The method as recited in claim 14, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

16. The method as recited in claim 11, wherein the delay is for allowing quarantining of the potentially malicious content until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

17. A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications; and

(d) delivering the network communications over the network in response to a request from a user.

18. The method as recited in claim 17, wherein the user is an intended recipient of the quarantined network communications.

19. The method as recited in claim 17, further comprising scanning the network communications for known malicious content.

20. The method as recited in claim 17, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

21. The method as recited in claim 17, wherein the network communications include electronic mail messages.

22. The method as recited in claim 21, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

23. A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring incoming and outgoing network communications over a network at a gateway;

(b) scanning the network communications for known malicious content;

(c) identifying potentially malicious content in the network communications;

(d) wherein content is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value;

(e) wherein the network communications include electronic mail messages, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line passing through the network for a given period of time is greater than a predetermined value;

(f) quarantining the potentially malicious content of the network communications;

(g) delivering the network communications over the network upon occurrence of the first of:

(i) scanning the potentially malicious content with a malicious code detection file received after the potentially malicious content is received;

(ii) upon receiving a user request;

(iii) upon passage of a predetermined amount of time;

(h) notifying an intended recipient of the potentially malicious content that the potentially malicious content has been quarantined;

(i) notifying a sender of the potentially malicious content that the potentially malicious content has been quarantined; and

(j) cleaning the potentially malicious content if malicious code is found for disabling the malicious code.